Remarks/Arguments

Claims 1-8, 10, 14, and 17-24 are pending. Claims 21-24 have been added to more fully claim the subject matter to which applicants believe they are entitled. In particular, the new claims relate to the method for processing a program signal having re-encrypted descrambling key information by an apparatus coupled to an access device in a local network. The steps of the method substantially correspond to those performed by, for example, the second device recited in claim 1. No new matter is believed to be added by new claims 21-24.

Prosecution on the application has been reopened by the outstanding Office Action in view of applicants' Appeal Brief filed on August 22, 2006. Applicants believe that the previously pending claims are patentably distinguishable over the cited prior art references for the reasons previously discussed; and that the newly cited reference does not add anything further. However, applicants submit the present response to more fully discuss the new reference cited by the examiner and to add new claims to which applicants believe they are entitled.

Previously, independent claim 1 was rejected under 35 USC 102 (e) in view of Tsuria (US Pat No 6178242 B1), and independent claims 10 and 17 were rejected under 35 USC 103(a) in view of Tsuria and Wasilewski (US Pat No 5870474). The examiner has now rejected all three independent claims under 35 USC 103 (a) in view of Tsuria and En-Seung (US Pat No 6892306). For the reasons discussed below, applicants submit that present independent claims 1, 10, and 17, and the claims that depend therefrom, are patentably distinguishable over the cited combination of Tsuria and En-Seung.

At the outset, applicants would like to point out that the examiner continues to misapply the teachings of Tsuria to the claimed invention. That is, the examiner continues to allege that the second device recited in claims 1 and 10, and the presentation device recited in claim 17, correspond to the VCR 130 disclosed by Tsuria. As discussed in previous responses and the Appeal Brief, applicants submit that such an allegation simply is not supported by the teachings or Tsuria.

The applicants have discussed in ample detail portions of Tsuria that simply do not support such an allegation, and maintain that the VCR 130 cannot properly be equated to the recited second device, or presentation device, for the reasons stated previously.

The examiner, in applying a rejection under 35 USC 103 (a), now curiously states that "Tsuria does not explicitly disclose receiving in said second device, said rebundled descrambling key." In fact, this statement also does not appears to be supported by Tsuria, given that Tsuria mentions generating a "recording SDDS", wherein the ECM is replaced with a TECM, see for example, col. 8, lines 16-19, and then shows in Fig. 1 that a recording format SDDS is applied to VCR 130. Thus, leaving aside the question of whether VCR 130 can correspond to the recited second device, or presentation device, Tsuria discloses that the VCR 130 does receive a data stream that includes the TECM, which is alleged to correspond to the rebundled descrambling key, and again the examiner's interpretation of Tsuria is not in fact supported by the teachings of Tsuria.

In any event, the examiner attempts to cure the alleged defect of Tsuria by citing En-Seung. However, applicants submit that even assuming arguendo that VCR 130 corresponds to the recited second device, or presentation device, and Tsuria and En-Seung can be combined in the manner suggested, the present independent claims 1, 10 and 17 are still patentably distinguishable over the cited combination because the combination fails to teach or suggest each and every limitation of the independent claims.

In the present invention, the rebundling of the descrambling key is performed using **a key associated with the access device**. That is, independent claim 1 recites "... rebundling, in said first device, said descrambling key using a unique key associated with said first device," claim 10 recites "... re-encrypting said descrambling key, in said access device, using a public key associated with said access device," and claim 17 recites "...an encryption unit for re-encrypting the descrambling key using a public key associated with the access device." By contrast, En-Seung describes an arrangement in which the **validation key is encrypted using the user key**, that is, the key associated with terminal unit 20.

In the Office Action, the examiner states that the ""rebundled descrambling key' is considered as an 'encrypted content key' and the content key is considered as a temporary validation key that encrypts the digital content and this content key is further encrypted by the user key associated with a PC computer for replaying the digital content." In fact, En-Seung discusses the use of three separate keys (Col. 4, lines 46-51). The first key is key information that is associated with a specific user and is used to generate the temporary validation key (col. 4, line 52 – col. 5, line 5). The second key is the user key that is used to encrypt and decrypt the temporary validation key (col. 5, lines 6-8). The third key is the temporary validation key that is used for encrypting the digital content and the header (col. 5, lines 28-31). Thus, the **user key is used to decrypt the temporary validation key**, which is used to decrypt the digital content (col. 22-24).

In the arrangement of En-Seung, the user keys are those keys associated with terminal unit 10. The examiner associates the features of terminal unit 10 with VCR 130 of Tsuria, which is alleged to correspond to the recited second device. If the arrangement of Tsuria is combined with the arrangement of En-Seung, as suggested by the examiner, the resulting combination would then result in the VCR 130 receiving a data stream having a rebundled descrambling key, which is rebundled using a key associated with the terminal unit, or second device, namely the VCR 130. Such a combination still fails to teach or suggest a rebundled descrambling key that is rebundled using a key associated with a first device, or access device, as recited in independent claims 1, 10 and 17.

Therefore, applicants submit that the combination fails to teach or suggest at least the steps of receiving in the second device a scrambled data component and a rebundled descrambling key and obtaining in the second device the descrambling key from the rebundled descrambling key as recited in claim 1. Also, the suggested combination fails to teach or suggest receiving in the presentation device the scrambled data component and the re-encrypted descrambling key and decrypting in the presentation device the re-encrypted descrambling key to obtain the descrambling key as recited in claim 10. Also, the suggested combination fails to teach or suggest a signal output coupled to a digital bus for transmitting the scrambled data component and the re-encrypted descrambling key to a presentation device via the digital bus, wherein only a presentation device having a corresponding private key is able to decrypt the re-encrypted descrambling key and descramble the scrambled content.

Further, applicants submit that the suggested combination of Tsuria and En-Seung is improper since neither reference teaches or suggests the desirability or such a combination. Tsuria and En-Seung are directed to entirely different problems and provide different solutions to address their respective problems.

Tsuria is directed to the specific problem that an apparatus may be unable to process a recorded scrambled signal if the security card having the descrambling information is changed subsequent to the recording. Tsuria address the problem by providing an apparatus that changes the descrambling key data included with the data stream with descrambling key data that is associated with the access device and will not subsequently be changed, even if the security card associated with the apparatus is changed.

En-Seung, by contrast, relates to a general problem of copy protection and the use of keys in the transmission and replay of digital information. En-Seung does not recognize or is remotely concerned with the problem or solution addressed by Tsuria, and thus, provides a completely different solution.

In fact, the arrangements of Tsuria and En-Seung appear to relate to entirely different environments. Tsuria relates to recording and processing within a local network environment, that is, **after** the user has received the signal from the broadcaster, or service provider. En-Seung, by contrast, relates to a processing arrangement including a service provider, wherein service server 22, encrypts and transmits digital content to one of a plurality of users, terminal unit 20, that have requested the digital content. This view is consistent with the fact that En-Seung teaches the use of user keys associated with specific users to encrypt the temporary validation key, while Tsuria discloses generating TECM based on the access device. The examiner's generalized statements regarding the fact that Tsuria relates to a protection mechanism and En-Seung relates to an improved and more efficient cryptographic process fails to take into account the actual specific arrangements, and problems addressed by the respective references. The Office Action simply fails to point to any portions of either reference that teaches or suggests the proposed combination. Thus, Applicants submit that nothing in either Tsuria or En-Seung teaches or suggests combining the references in the manner suggested by the examiner.

In view of the above, applicants submit that claims 1, 10 and 17, and the claims that depend therefrom, are patentably distinguishable over the suggested combination of Tsuria and En-Seung.

New claims 21-24 recite "... receiving, from an access device in a local network and coupled to a service provider, a signal comprising the program signal in scrambled form and a re-encrypted descrambling information, the descrambling information being re-encrypted by the access device using key information associated with the access device..." and are believed to be patentably distinguishable over the combination of Tsuria and En-Seung for at least the same reasons as those discussed above with respect to claims 1, 10 and 17.

Rejection of claims 6 and 18 in view of Tsuria, En-Seung, and Wasilewski

The examiner states that Tsuria as modified does not expressly disclose initializing comprising the step of receiving a public key from a conditional access provider as recited in claim 6, nor that the public key is periodically received from a conditional access provider as recited in claim 18. Wasilewski is cited to provide the missing elements of the Tsuria as modified. Applicants submit that even assuming arguendo that Wasilewski provides the missing elements, Wasilewski still fails to cure the defect of Tsuria and En-Seung as discussed above, and as such, claims 6 and 18, which depend from claims 1 and 17, respectively, are patentably distinguishable over the suggested combination.

Rejection of claim 19 in view of Tsuria, En-Seung and Smyers

The examiner states that Tsuria as modified does not teach a signal output authenticates the presentation device before transmitting the scrambled data component and the re-encrypted descrambling key to the presentation devices. Smyers is cited to provide the missing elements of Tsuria as modified. Applicants submit that even assuming arguendo that Smyers provides the missing elements, Smyers fails to cure the defect of Tsuria and En-Seung as discussed above, and as such, claim 19, which depends from claim 17, is patentably distinguishable over the suggested combination.

Conclusion

Having fully addressed the Examiner's rejections it is believed that, in view of the preceding amendments and remarks, this application stands in condition for allowance. Accordingly then, reconsideration and allowance are respectfully solicited. If, however, the Examiner is of the opinion that such action cannot be taken, the Examiner is invited to contact the applicants' attorney at (609) 734-6815, so that a mutually convenient date and time for a telephonic interview may be scheduled.

Respectfully submitted,
AHMET MURSIT ESKICIOGLU, ET AL.

By: Paul P. Kiel
Attorney for Applicants
Registration No. 40,677
Phone No. 609-734-6815

THOMSON Licensing LLC
PO Box 5312
Princeton, NJ 08543-5312

Date: 2/7/07